12. LeCun Y., Bottou L., Bengio Y., Haffner P. Gradient-Based Learning Applied to Document Recognition *Proceedings of the IEEE*. 1998, vol. 86, no. 11, pp. 2278–2324.
13. Kahou S, Bouthillier X., Lamblin P. EmoNets: Multimodal deep learning approaches for emotion recognition in video. *Journal on Multimodal User Interfaces*. 2015, no. 10, pp. 99–111.
14. *Challenges in Representation Learning: Facial Expression Recognition Challenge*. Available at: https://www.kaggle.com/c/challenges-in-representation-learning-facial-expression-recognition-challenge/data (accessed 12.03.2020).

Поступила (received) 16.04.2020

Відомості про авторів / Сведения об авторах / About the Authors

Ульянко Артем Леонідович – Національний технічний університет «Харківський політехнічний інститут», аспірант кафедри системного аналізу та інформаційно-аналітичних технологій, м. Харків, Україна; ORCID: 0000-0003-3278-2687; e-mail: artem.ulyanko@gmail.com.

Дорофєєв Юрій Іванович (***Дорофеев Юрий Иванович***, ***Dorofieiev Yuri Ivanovych***) – доктор технічних наук, професор, Національний технічний університет «Харківський політехнічний інститут», професор кафедри системного аналізу та інформаційно-аналітичних технологій; м. Харків, Україна; ORCID: 0000-0002-7964-1286; e-mail: dorofeev@kpi.kharkiv.edu.

Ульянко Артем Леонидович – Национальный технический университет «Харьковский политехнический институт», аспирант кафедры системного анализа и информационно-аналитических технологий, г. Харьков, Украина; ORCID: 0000-0003-3278-2687; e-mail: artem.ulyanko@gmail.com.

Дорофеев Юрий Иванович – доктор технических наук, профессор, Национальный технический университет «Харьковский политехнический институт», профессор кафедры системного анализа и информационно-аналитических технологий; г. Харьков, Украина; ORCID: 0000-0002-7964-1286; e-mail: dorofeev@kpi.kharkiv.edu.

Ulianko Artem Leonidovych – National Technical University "Kharkiv Polytechnic Institute", graduate student of the Department of System Analysis and Information-Analytical Technologies; Kharkiv city, Ukraine; ORCID: 0000-0003-3278-2687; e-mail: artem.ulyanko@gmail.com.

Dorofieiev Yuri Ivanovych – Doctor of Technical Sciences, Professor, National Technical University "Kharkiv Polytechnic Institute", Professor of the Department of System Analysis and Information-Analytical Technologies; Kharkiv city, Ukraine; ORCID: 0000-0002-7964-1286; e-mail: dorofeev@kpi.kharkiv.edu.

УДК 004.02 **DOI: 10.20998/2079-0023.2020.01.16**

Є. Л. БАТУРІН, В. Ю. ВОЛОВЩИКОВ, В. Ф. ШАПО

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДСИСТЕМИ ІДЕНТИФІКАЦІЇ НА ОСНОВІ ЕЛЕКТРОННИХ КЛЮЧІВ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

В роботі розглянуто проблему ідентифікації документів в системах електронного документообігу. Актуальність даної теми обґрунтовано широким використанням систем електронного документообігу які потребують надійної ідентифікації документів, що передаються. Основними проблемами для ідентифікації документів в системах електронного документообігу є необхідність підтвердження авторства, незмінності документу та встановлення часу підпису. Наведено огляд основних методів ідентифікації, встановлено їх переваги та недоліки. Після аналізу можливих методів ідентифікації встановлено, що метод оснований на використанні електронних ключів дозволяє надійно встановити авторство документа, надає можливість встановити час підпису, забезпечує безвідмовність факту підпису та не потребує значних ресурсів для його формування та перевірки. Це принципово виділяє метод ідентифікації на основі електронних ключів серед інших. В основу метода покладено алгоритм цифрового підпису еліптичної кривої. Стійкість обраного алгоритму ґрунтується на проблемі дискретного логарифма в групі точок еліптичної кривої. Для реалізації алгоритму використовуються відкритий та закритий ключі. Після генерації пари ключів закритий ключ зберігається користувачем в таємниці та використовується для підпису документів, а відкритий використовується для ідентифікації користувача та має бути відомий всім користувачам системи. Розглянуто інформаційну підтримку підсистеми ідентифікації. Запропонована трирівнева архітектурна модель в якій роль клієнтського рівня виконує прикладний програмний інтерфейс. Обґрунтовано технології реалізації алгоритму підпису. Описані основні модулі, з яких має складатися підсистема та їх зв'язки. Розроблено програмне забезпечення підсистеми ідентифікації, яке дозволяє користувачам створювати як окремий так і вбудований в документ підпис а також виконувати його перевірку. Розроблена підсистема ідентифікації протестована з використанням файлів різних форматів та розмірів.

Ключові слова: підсистема ідентифікації, електронні ключі, документообіг, електронний підпис, алгоритм цифрового підпису еліптичної кривої, ідентифікація документа.

Е. Л. БАТУРИН, В. Ю. ВОЛОВЩИКОВ, В. Ф. ШАПО

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ПОДСИСТЕМЫ ИДЕНТИФИКАЦИИ НА ОСНОВЕ ЕЛЕКТРОННЫХ КЛЮЧЕЙ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

В работе рассмотрена проблема идентификации документов в системах электронного документооборота. Актуальность данной темы обоснована широким использованием систем электронного документооборота требующих надежной идентификации передаваемых документов. Основными проблемами для идентификации документов в системах электронного документооборота являются необходимость подтверждения авторства, неизменности документа и определение времени подписи. Приведен обзор основных методов идентификации,

установлены их достоинства и недостатки. После анализа возможных методов идентификации установлено, что метод, основанный на использовании электронных ключей, позволяет надежно установить авторство документа, установить время подписи, обеспечивает безотказность факта подписи и не требует значительных ресурсов для её формирования и проверки. Это принципиально выделяет метод идентификации на основе электронных ключей среди других. В основу метода положен алгоритм цифровой подписи эллиптической кривой. Устойчивость избранного алгоритма основывается на проблеме дискретного логарифма в группе точек эллиптической кривой. Для реализации алгоритма используются открытый и закрытый ключи. После генерации пары ключей закрытый ключ хранится пользователем в тайне и используется для подписи документов, а открытый используется для идентификации пользователя и должен быть известен всем пользователям системы. Рассмотрена информационная поддержка подсистемы идентификации. Предложена трехуровневая архитектурная модель, в которой роль клиентского уровня выполняет прикладной программный интерфейс. Обоснованы технологии реализации алгоритмов подписи. Описаны основные модули, из которых должна состоять подсистема и их связи. Разработано программное обеспечение подсистемы идентификации, которое позволяет пользователям создавать как отдельную, так и встроенную в документ подпись, а также выполнять её проверку. Разработанная подсистема идентификации протестирована с использованием файлов различных форматов и размеров.

Ключевые слова: подсистема идентификации, электронные ключи, документооборот, электронная подпись, алгоритм цифровой подписи эллиптической кривой, идентификация документа.

Y. L. BATURIN, V. Y. VOLOVSHCHYKOV, V. F. SHAPO

INFORMATION TECHNOLOGY OF THE IDENTIFICATION SUBSYSTEM BASED ON ELECTRONIC KEYS IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

The paper considers the problem of documents identification in electronic document management systems. The relevance of this topic is justified by the widespread use of electronic document management systems which require reliable identification of transferred documents. The main problems for identifying documents in electronic document management systems are authorship confirmation, confirmation of the document immutability and determining the signing time. A review of the main methods of identification is given, their advantages and disadvantages are identified. After possible identification methods analyzing, it was found that the method based on the electronic keys allows to reliably identify the document, determine the signing time, guaranty the fact of signing and does not require significant amount of resources for sign formation and verification. This distinguishes the method of identification based on electronic keys fundamentally among others. The method is based on the elliptic curve digital signature algorithm. The reliability of the chosen algorithm is based on the problem of the discrete logarithm in the group of points of the elliptic curve. To implement the algorithm public and private keys are used. After generating a key pair, the private key is kept in secret by the user and used to sign documents, the public key is used to identify the user and should be known to all users of the system. The information support of the identification subsystem is provided. A three-level architectural model in which the client level role is performed by the application programming interface is proposed. The technologies for implementing signature algorithms are considered. Identification subsystem software has been developed. This software allows users to create both individual and built-in document signatures, as well as to verify it. The developed identification subsystem was tested using files of different formats and sizes.

Keywords: identification subsystem, electronic keys, document flow, electronic signature, elliptic curve digital signature algorithm, document identification.

Вступ. Наявні способи передачі та обробки інформації обумовили появу загроз, пов’язаних з втратою, зміною або розкриттям даних. Це призвело до розвитку напряму інформаційної безпеки комп'ютерних систем і мереж. Під інформаційною безпекою розуміють захищеність інформації від несанкціонованого ознайомлення, зміни та знищення, а також захищеність інформаційних ресурсів від дій, спрямованих на порушення їх працездатності [1]. Інформаційна безпека комп'ютерних систем досягається гарантією конфіденційності, цілісності та достовірності даних, що обробляються, а також доступності та цілісності інформаційних компонентів і ресурсів системи.

Для контролю доступу до інформації та ресурсів системи, а також забезпечення цілісності та достовірності даних використовуються підсистеми ідентифікації та аутентифікації [1–3]. Це робить розробку підсистем ідентифікації та аутентифікації актуальним та важливим напрямом.

Проблема ідентифікації учасників електронної взаємодії. Те, що наразі питання розробки підсистем ідентифікації та аутентифікації є актуальними доводить все більша увага науковців в галузі інформаційної безпеки. Способи ідентифікації та аутентифікації учасників електронної взаємодії всебічно розглядаються та класифікуються в багатьох публікаціях. Насамперед слід відмітити, що на основі аналізу [1, 3] можна стверджувати, що поняття ідентифікації та аутентифікації є взаємопов’язаними та виконують функцію перевірки справжності суб’єктів. Тож має сенс розглядати їх як єдине поняття ідентифікації. Слід зауважити, що підсистеми ідентифікації можуть бути класифіковані за різними ознаками. Так, наприклад, в роботах [1, 4, 5] автори категоризують підсистеми ідентифікації за типом наданих суб’єктом сутностей.

1. Ідентифікуючі користувача за тим, що він знає. До таких підсистем автори відносять парольні підсистеми та ті, що засновані на PIN-кодах.

2. Ідентифікуючі користувача за тим, що він має. Прикладом є смарт-картки, електронні ключі, магнітні картки.

3. Ідентифікуючі користувача за тим, хто він є. Такі підсистеми засновані на фізіологічних та поведінкових атрибутах живого організму.

Зі свого боку роботи [1, 6] надають наступну класифікацію підсистем ідентифікації за різновидами використаних ідентифікаційних ознак.

1. Електронні. В таких підсистемах ознаки ідентифікації зберігаються в пам’яті у вигляді цифрового коду ідентифікатора.

2. Біометричні. Такі підсистеми для роботи використовують унікальні особливості людини в якості ідетифікаторів. В роботах виділяються статична та динамічна біометрії. Статична біометрія заснована на вимірюванні фізіологічних особливостей людини в той час як динамічна біометрія заснована на аналізі дій та поведінки людини.

3. Комбіновані. Згідно з аналізом джерел такі системи використовують одночасно декілька ознак для ідентифікації.

Таким чином, можна стверджувати, в тому числі спираючись на аналіз [1, 3–6], що проблема ідентифі-

кації наразі активно розглядається багатьма як вітчизняними, так і іноземними авторами, та потребує вирішення.

Аналіз існуючих методів. Одним з методів надійної ідентифікації є парольна ідентифікація. В роботах [1–3] детально розглядаються парольні підсистеми ідентифікації. Ці підсистеми можуть базуватися на одноразових та багаторазових [1, 2] паролях. Процедура ідентифікації користувача за допомогою багаторазового пароля може бути описана наступним чином. Користувач надає системі свої ідентифікатор і пароль. Вони надходять для обробки на сервер ідентифікації. У базі даних, що зберігається на сервері ідентифікації, за ідентифікатором користувача знаходиться відповідний запис, з нього витягується хеш пароля і порівнюється з хешем наданого пароля. Якщо вони співпали, то ідентифікація пройшла успішно, користувач отримує права і ресурси мережі, які визначені для його статусу. Одноразові паролі найчастіше можуть бути використані в системах двофакторної ідентифікації. В такому разі користувачеві або пристрою необхідно пред'явити одноразовий пароль, згенерований центром розподілу паролей. Для забезпечення надійного захисту пароль повинен бути відомий лише користувачеві та нікому іншому. Автори відмічають такі переваги метода як простота використання та легкість інтеграції. Всі наведені роботи зазначають низьку надійність методу. Одним з найсуттєвіших недоліків є залежність надійності методу від користувачів [3].

Джерела [7–10] описують статичні біометричні підсистеми ідентифікації за голосом, обличчям та відбитками пальців. Технологія сканування обличчя підходить для тих випадків, де інші біометричні технології непридатні [7, 8]. Для ідентифікації особистості система використовує особливості очей, носа та губ. Процес аналізу ідентифікаторів зазвичай є ресурсномістким та виконується за допомогою систем штучного інтелекту. Основна перевага такого методу полягає в тому, що ідентифікація може проходити без прямої участі людини в її процесі. Такі системи широко використовуються в місцях великого скупчення людей. Однак вони не позбавлені недоліків. Наприклад, висуваються суворі вимоги до апаратів, що створюють зображення а також до самого зображення. До того ж на якість ідентифікації суттєво впливає освітленість.

Іншим прикладом біометричної системи ідентифікації є ідентифікація користувача за голосом, яка спирається на висоту, модуляцію та частоту звуку [9]. Технології розпізнавання за голосом мають деякі обмеження: голос людини можна легко записати, він змінюється залежно від самопочуття, емоційного стану та віку людини. Це обмежує використання даного метода здебільшого системами телефонії [1].

Метод встановлення особи за відбитком пальця, також відомий як дактилоскопія, є найбільш поширеним методом статичної біометричної ідентифікації [10]. Суть методу полягає в наступному: користувач прикладає палець до спеціального сканера, потім отримані дані про відбиток пальця перетворюються в цифровий код і порівнюються з кодами, наявними в базі даних системи ідентифікації. Застосування методу засноване на факті унікальності малюнка папілярних візерунків. Однією з основних причин широкого розповсюдження цього методу є наявність великих банків даних відбитків пальців. У загальному випадку підсистема ідентифікації на основі розпізнавання відбитків пальців замінює парольну підсистему ідентифікації.

В роботах [11, 12] розглядається питання динамічної біометричної ідентифікації. Одним з варіантів підсистеми ідентифікації на основі динамічної біометрії є підсистема ідентифікації на основі аналізу поведінки користувача в мережі [11]. Шляхом аналізу мережевого трафіку виявляються особливості кожного користувача, які виступають в якості ідентифікаторів. Аналізу піддаються як використані доменні імена, так і динаміка їх використання. Аналізується кількість запитів та їх інтенсивність а також використані інтернет додатки. Даний метод дуже вразливий до атак. Загалом надійність метода обумовлена збереженням в секреті алгоритмів аналізу. На практиці даний метод використовується лише як додатковий засіб захисту в комбінованих підсистемах ідентифікації.

Ще одним засобом динамічної біометричної ідентифікації користувача є аналіз клавіатурного почерку [12]. Клавіатурний почерк характеризують швидкість та динаміка введення а також частота виникнення помилок та використання клавіш. Автор розрізнює спосіб ідентифікації за введенням відомої та невідомої фрази. Обидва способи включають в себе режим навчання та режим ідентифікації. В режимі навчання система формує еталонні зразки з якими надалі буде зіставляти отримані дані. В режимі ідентифікації система з заданою періодичністю отримує інформацію про клавіатурний почерк користувача та, зіставляючи його з еталоном, робить висновок про надання доступу до ресурсів. Метод може працювати в фоновому режимі, тим самим забезпечуючи ідентифікацію користувача впродовж всієї робочої сесії. Недоліком методу аналізу клавіатурного почерку є обмеження областей використання підсистеми та низька надійність.

Деякі роботи [1, 13] висвітлюють проблему використання підсистем суворої ідентифікації. Так, автори одночасно вказують на те, що процедури суворої ідентифікації поділяються на односторонню, двосторонню та тристоронню ідентифікацію. Одностороння ідентифікація передбачає обмін інформацією лише в одному напрямі. Даний тип ідентифікації дозволяє виконати низку операцій.

1. Підтвердити справжність тільки однієї сторони інформаційного обміну.

2. Виявити порушення цілісності інформації, що передається.

3. Гарантувати, що переданими даними може скористатися лише сторона, що перевіряє.

Двостороння ідентифікація до того ж містить додаткову відповідь стороні, що перевіряє, яка повинна довести, що зв'язок встановлено з потрібним користувачем.

Тристороння сувора ідентифікація містить додаткову передачу даних від сторони, що доказує до

сторони, що перевіряє. Це дозволяє відмовитися від використання міток часу.

Також в проаналізованих роботах мова йде про те, що підсистеми суворої ідентифікації, в залежності від алгоритму, що використовується, поділяються на декілька груп.

1. Засновані на симетричних алгоритмах шифрування.
2. Засновані на алгоритмах електронного цифрового підпису.
3. Засновані на використанні криптографічного контрольного значення.
4. Засновані на нульових знаннях.
5. Засновані на сертифікатах з використанням перетворень в групах точок еліптичної кривої.

В більшості випадків сувора ідентифікації засновується на механізмі електронних ключів. Користувач має можливість визначити, чи володіє його партнер по зв'язку належним секретним ключем і чи може він використовувати цей ключ для підтвердження того, що він дійсно є справжнім партнером по інформаційному обміну.

Проаналізувавши матеріал, можна відмітити високу надійність, можливість гарантувати захист даних від стороннього втручання а також можливість підтвердження авторства переданих даних як відмінну рису підсистем суворої ідентифікації. Специфікою використання даного типу підсистем є області, де потрібно ідентифікувати автора даних, що передаються, а також впевнитися в цілісності цих даних та забезпечити неможливість відмови від факту передачі даних.

Постановка задачі. Аналіз робіт [1–13] показав, що наразі широко вивчаються різні підсистеми ідентифікації та підходи до їх реалізації. Також аналіз показав наявність областей, що потребують вирішення проблеми ідентифікації. Виходячи з цього, процес розробки підсистеми ідентифікації є актуальним.

На основі аналізу [14, 15] можна стверджувати, що проблема ідентифікації в системах електронного документообігу на даний час є актуальною. Також в роботах описані основні вимоги до підсистем ідентифікації, які мають бути задоволені для забезпечення всіх потреб інформаційної безпеки систем електронного документообігу. До таких вимог відносять надійність ідентифікації, можливість встановити авторство даних, та гарантувати неможливість відмови відправника від факту передачі даних. Для вирішення задачі ідентифікації в роботі пропонується використання підсистеми ідентифікації на основі електронних ключів. На основі аналізу існуючих методів ідентифікації можна стверджувати, що тільки ця підсистема в повній мірі задовольняє вимогам до підсистем ідентифікації обраної предметної області.

Таким чином, метою роботи є побудова інформаційної технології підсистеми ідентифікації на основі електронних ключів.

Концептуальна модель підсистеми ідентифікації на основі електронних ключів. Підсистема ідентифікації повинна забезпечувати можливість ідентифікації електронних документів будь-яких форматів за допомогою електронного цифрового підпису. В роботі розглядаються питання формування та перевірки електронного цифрового підпису з використанням електронних ключів. Пара приватного та публічного ключів генерується окремо для кожного з користувачів підсистеми. Приватний ключ повинен триматися в таємниці та зберігатися в локальному сховищі електронних ключів для подальшого його використання при підписанні електронних документів. Зі свого боку відкритий ключ має зберігатися в базі даних підсистеми ідентифікації та бути доступним всім користувачам підсистеми при використанні для перевірки дійсності підпису. Тоді процес підпису документа користувачем полягатиме в завантаженні документа та приватного ключа до підсистеми ідентифікації та вибору варіанту підписання. Автори вважають, що при цьому актуальним є один з двох сценаріїв генерації підпису.

1. Генерація підпису окремо від документа.
2. Генерація підпису вбудованого в документ.

Зворотній процес, який полягає в перевірці підпису, повинен також бути реалізований в межах підсистеми ідентифікації. В цьому випадку користувач має завантажити в підсистему підписаний документ або підпис та документ окремо.

Таким чином, цілісна підсистема ідентифікації повинна являти собою сукупність пов’язаних між собою програмних модулів. Модуль управління обліковими записами користувачів має надавати системі вищого рівня можливість зберігати та обробляти інформацію про користувачів підсистеми. Для надання функціоналу генерації пар публічних і приватних електронних ключів в підсистемі має бути реалізований модуль генерації електронних ключів. Модуль формування електронного цифрового підпису повинен надавати функціональність, що дозволятиме, отримавши в якості вихідних даних документ та приватний ключ, зберегти підписаний документ або підпис окремо від документа. Для отримання інформації щодо дійсності наданого підписаного документа або підпису окремо від документа підсистема повинна мати модуль перевірки електронного цифрового підпису.

Один з варіантів використання підсистеми ідентифікації – це генерація та зберігання користувачем приватного ключа та електронного цифрового підпису на автоматизованому робочому місці (АРМ) за допомогою надсилання відповідних запитів до підсистеми ідентифікації з web-браузера. В подальшому виконується передача підписаного документу транспортним каналом іншому користувачу, який за допомогою web-браузера надсилає запит на перевірку підпису. Концептуальна модель підсистеми ідентифікації зображена на рис. 1.

Технологія формування електронного цифрового підпису. Для формування електронного цифрового підпису в статті пропонується використання алгоритму Elliptic Curve Digital Signature Algorithm [1]. На першому етапі формування електронного цифрового підпису для документа M обчислюється його хеш-код

$$\bar{h} = h(M),$$

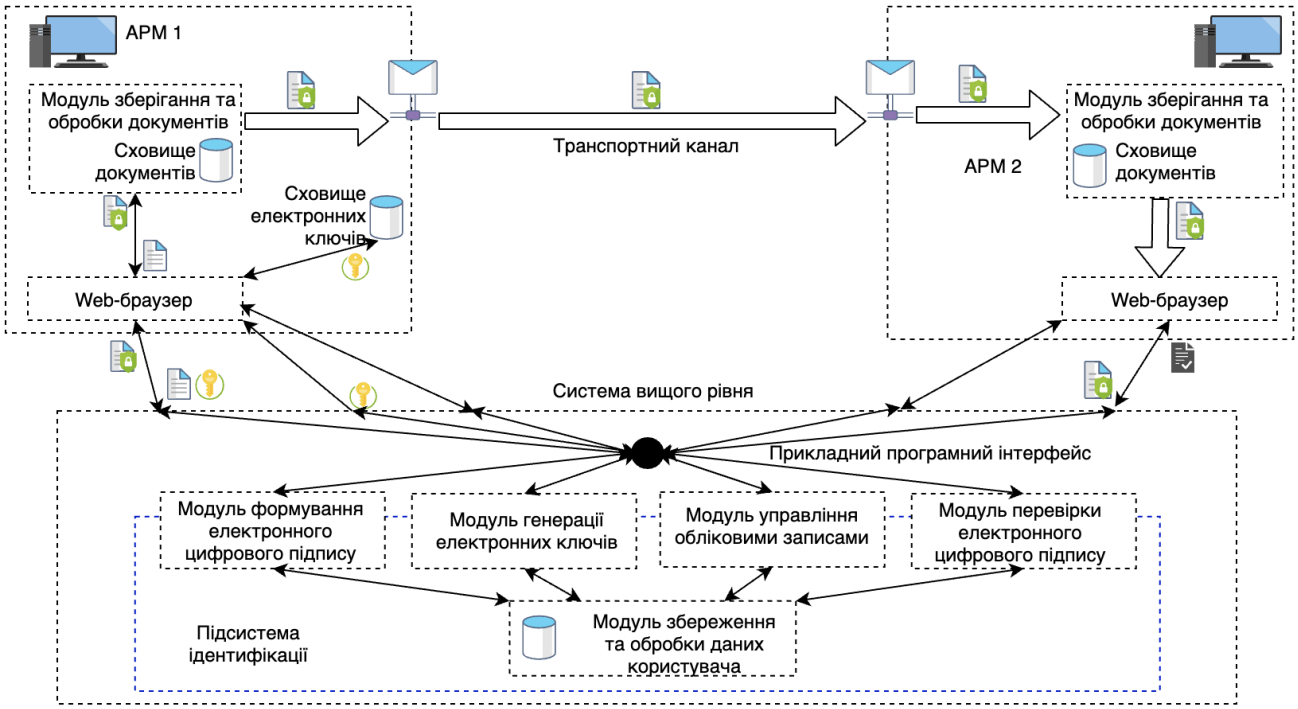

Рис. 1. Концептуальна модель підсистеми ідентифікації

а також ціле число α, двійковим представленням якого є вектор $\bar{h}$, та обчислюється

$$e = \alpha(\mathrm{mod}\ q),$$

де q – велике просте число що представляє порядок підгрупи групи точок еліптичної кривої для якого виконуються наступні умови:

$$\begin{cases} m = nq, n \in Z, n \geq 1, \\ 2^{254} < q < 2^{256}, \end{cases}$$

де m – ціле число, порядок групи точок еліптичної кривої.

Якщо $e = 0$, то визначається $e = 1$.

Другий етап починається з генерації випадкового (псевдовипадкового) цілого числа k, такого, що задовільнить нерівності

$$0 < k < q.$$

Також обчислюється точка еліптичної кривої:

$$C = kP,$$

де $P \neq 0$ – точка еліптичної кривої з координатами (x_p, y_p), що задовольняє рівності $qP = 0$.

Сутність третього етапу полягає в обчисленні

$$r = x_r(\mathrm{mod}\ q),$$

де x_r – x координата точки C.

Якщо $r = 0$, то слід повернутися до другого етапу алгоритму.

На четвертому етапі визначається значення

$$s = (rd + ke)(\mathrm{mod}\ q),$$

де d – ціле число, задовольняє нерівності $0 < d < q$.

Якщо $s = 0$ то алгоритм повторюється з другого етапу.

П'ятий етап починається з обчислення двійкових векторів $\bar{r}$ та $\bar{s}$ що відповідають r та s, визначається цифровий підпис як конкатенація двох двійкових векторів

$$\varpi = (\bar{r}||\bar{s}).$$

Для перевірки електронного цифрового підпису $(\bar{r}||\bar{s})$ на першому етапі з отриманого підпису обчислюються цілі числа r та s. Якщо виконуються нерівності:

$$0 < r < q,$$

$$0 < s < q,$$

то обчислення продовжується, інакше – підпис вважається невірним.

Другий етап починається з обчислення хеш-коду отриманого документа M

$$\bar{h} = h(M),$$

також обчислюється ціле число α, двійковим представленням якого є вектор $\bar{h}$, визначається

$$e = \alpha(\mathrm{mod}\ q).$$

Якщо e $= 0$, визначається $e = 1$.

На третьому етапі обчислюються значення:

$$z_1 = s^{-1}\bar{h}(\mathrm{mod}\ q),$$

$$z_2 = -s^{-1}r(\mathrm{mod}\ q).$$

На останньому етапі обчислюється точка еліптичної кривої

$$C = z_1P + z_2Q,$$

та визначається:

$$R = x_r(\mathrm{mod}\ q),$$

де x_c – координати точки C. Якщо рівність $R = r$ виконано, то підпис вважається дійсним, інакше – підпис невірний.

Інформаційна підтримка підсистеми ідентифікації на основі електронних ключів. Для реалізації описаного функціоналу авторами пропонується трирівнева архітектурна модель [16], в якій роль клієнтського рівня виконується прикладним програмним інтерфейсом, а основна частина задач по обробці інформації в підсистемі покладається на сервер застосунку. Запити від системи вищого рівня через прикладний програмний інтерфейс передаються на логічний рівень архітектурної моделі – сервер застосунку підсистеми ідентифікації. В якості сервера застосунку пропонується використання apache tomcat [17] – промислового рішення з відкритим вихідним кодом. За допомогою ресурсів сервера застосунку обчислюються основні операції підсистеми а також здійснюватися доступ до рівня даних. На рівні даних пропонується використання реляційної системи керування базами даних MySql [18]. Загальна схема архітектури підсистеми ідентифікації зображена на рис. 2.

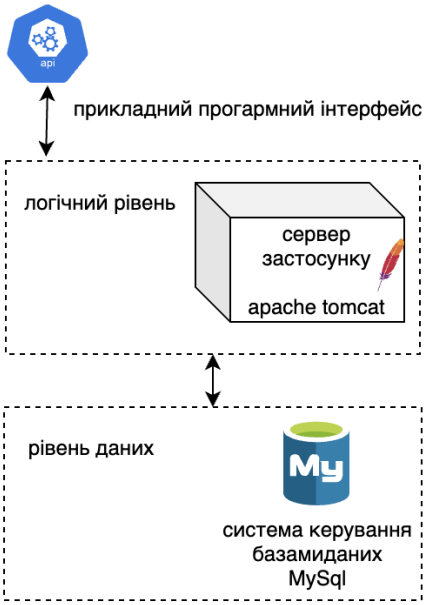

Рис. 2. Загальна схема архітектури підсистеми ідентифікації

З точки зору організації модулів програми мають бути відокремлені модулі, які використовують криптографічні функції для реалізації функціоналу, а саме: модуль формування електронного цифрового підпису, модуль перевірки електронного цифрового підпису та модуль генерації електронних ключів. Окремо слід виділити модуль відповідальний за обробку та збереження даних користувачів, який повинен мати доступ до бази даних. Клієнт повинен мати можливість взаємодіяти з рівнем даних лише через використання функціоналу логічного рівня. Діаграма компонентів підсистеми зображена на рис. 3.

Для імплементації підсистеми пропонується використання мови програмування Java [19]. В якості провайдера криптографічних функцій автори пропонують використання прикладного програмного інтерфейсу криптопровайдера з відкритим вихідним кодом Bounce Castle Crypto [20], який надає високорівневий інтерфейс для реалізації промислових стандартів Java Cryptography Extension [19] та Java Cryptography Architecture [19] з пакету Java Security [19] стандартної бібліотеки Java.

Результати досліджень. В результаті проведення дослідження отримано систему з прикладним інтерфейсом користувача, використовуючи який можна надсилати відповідні запити на генерацію ключів, підпис або перевірку підпису електронного документа.

В якості документа для підпису було використано файли різного розміру та формату. В таб. 1 наведено результати надсилання запитів з використанням документа формату rtf розміром 1 мегабайт. Табл. 2 демонструє результати однакових запитів на формування електронного цифрового підпису до системи з використанням документів різного формату та розміру.

Таблиця 1 – Результати запитів з використанням документу формату rtf розміром 1 мегабайт

Тип запиту	Час виконання	Результат
Запит на формування окремого від документа підпису	40–78 мілісекунд	Файл підпису розміром 793 байта
Запит на перевірку окремого від документа підпису	128–177 мілісекунд	Результат перевірки підпису в текстовому форматі
Запит на формування підпису вбудованого в документ	41–58 мілісекунд	Файл з вбудованим підписом розміром 1 мегабайт 793 байта.
Запит на перевірку підпису вбудованого в документ	117–143 мілісекунд	Результат перевірки підпису в текстовому форматі

Для зручності користувача передбачено інтерфейс для отримання статистичної інформації щодо документа, а саме: кількість підписань, кількість вдалих перевірок підпису, кількість невдалих перевірок підпису а також дату та час кожного підпису та інформацію щодо користувача-підписанта.

Висновки. В роботі розглянуто інформаційну технологію підсистеми ідентифікації на основі електронних ключів. В основу системи покладено трирівневу архітектурну модель в якій роль клієнта виконує прикладний програмний інтерфейс з використанням якого надається доступ до ресурсів підсистеми.

Таблиця 2 – Результати запиту на формування окремого підпису з використанням документів різного формату та розміру

Формат файла	Розмір файла	Час виконання
rtf	1 мегабайт	40–78 мілісекунд
mp4	446,3 мегабайта	10,28–11,43 секунд
pdf	228 кілобайт	28–34 мілісекунд

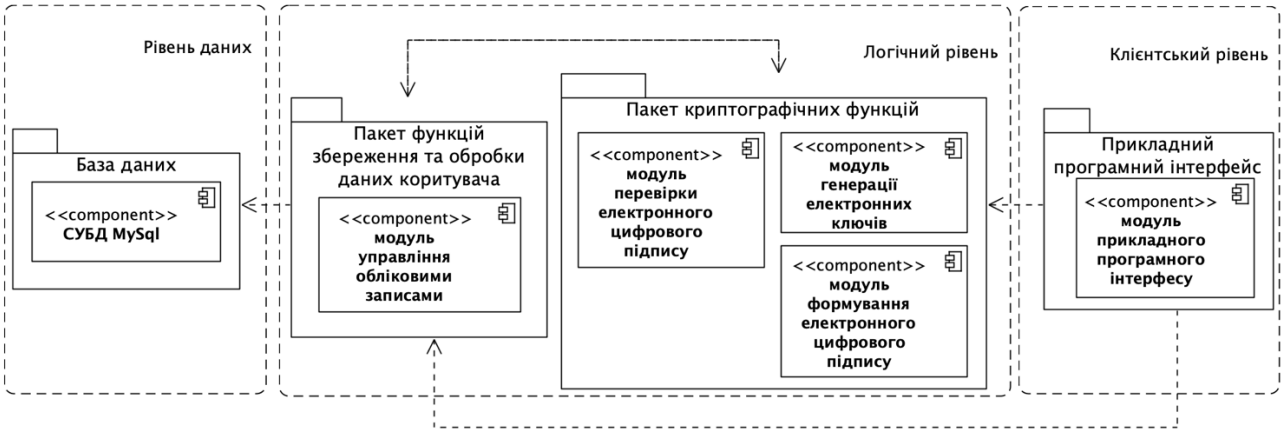

Рис. 3. Діаграма компонентів

Результатом дослідження є програмне забезпечення системи, яке виконує описані функції та відповідає висунутим вимогам. Розроблена підсистема надає функціональність для генерації пар електронних ключів а також підписання та перевірки підпису електронних документів будь-якого формату. Впровадження подібної підсистеми дозволить автоматизувати процес підпису документів що, зі свого боку, дасть можливість прискорити бізнес-процеси та підвищити надійність системи.

Список літератури

1. Шаньгин В. Ф. *Защита компьютерной информации. Эффективные методы и средства.* Москва: ДМК, 2010. 542 с.
2. Стельмашонок Е. В., Васильева И. Н. *Защита информации в компьютерных системах.* Санкт-Петербург: Из-во Санкт-Петербуржского нац. эконом. ун-та., 2017. 163 с.
3. Кошева Н. А., Мазніченко Н. І *Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів.* Харків: нац. ун-т «Юридична академія імені Ярослава Мудрого», 2013. Т. 113, № 6. С. 215–223.
4. Messaoud Benantar *Access Control Systems Security, Identity Management and Trust Models.* TX: Sringer Publ., 2003. 261p.
5. Марков А. С., Цирлов В. Л. Безопаснось доступа: подготовка к CISSP *// Вопросы кибербезопасности.* 2015. № 2. С. 60–68.
6. Фадюшин А. М., Симонов В. Л. Современные системы идентификации личности. *Современные информационные технологи в образовании, науке и промышленности (02–03 ноября 2018 г., Москва)*. Москва: Спутник, 2018. С. 176–178.
7. Максименко В. Н., Волошина Т. С. Анализ системы распознавания лиц по алгоритму нейронной сети. *// экономика и качество систем связи.* 2015. № 4. С. 31–37.
8. Горлов В. Н. Алгоритмические средства идентификации человека по фотопортрету на основе геометрических преобразований. *Сборник статей IV международно-научной конференции (20 сентября 2018 г., Пенза).* Пенза: МЦНО «Наука и просвещение», 2018. С. 23–27.
9. Брюхомицкий Ю. А., Федоров В. М. Метод текстонезависимой идентификаци личности по голосу // *Известия ЮФУ*. 2015. С. 173–181.
10. Калуцкий И.В., Матюшин Ю.С., Спевакова С.В. Анализ современных статических методов биометрической идентификации // *Известия Юго-Западного государственного университета*. 2019. Т. 23, № 1. С. 84–94.
11. Лихачев А. Е., Павловский Е. Н., Хазанкин Г. Р. Разработка системы идентификации пользователей компьютерных сетей на основе анализа их поведения. // *Транспортное дело*. 2017. С. 171.
12. Перегудов А. В. Клавиатурный почерк как дополнительный способ идентификации пользователя. Международная научно-практическая конференция «Научные исследования и современное образование» *(26 марта 2018 г. Владивосток)* Владивосток. 2018. С. 240–241.
13. Олешко И. В., Горбенко И. Д. Сравнительный анализ протоколов строгой аутентификации // *Радиоотехника 2018.* № 171 С. 198–209.
14. Сабанов А. Г. Аутентификация при электронном обмене конфиденциальными документами // *Доклады ТУСУРа.* 2011. Т. 22, № 2. С.267–270.
15. Макарова И.И. Комплексная информационная безопасность электронного документооборота // *Управління проектами та розвиток виробництва: Зб.наук.пр.* – Луганськ: вид-во СНУ ім. В.Даля, 2004. Т. 11. № 3. С.100-105.
16. Л. Басс, П. Клементс, Р. *Кацман Архитектура программного обеспечения на практике*. Санкт-Петербург: Из-во Addison-Wesley, 2006. 306 с.
17. Офіційний сайт Apache Tomcat / *онлайн документація* / URL: http://tomcat.apache.org (дата звернення: 11.05.2020).
18. Офіційний сайт MySql / *онлайн документація* / URL: http://mysql.com (дата звернення: 11.05.2020).
19. Офіційний сайт Java / *онлайн документація* / URL: http://java.com (дата звернення: 11.05.2020).
20. Офіційний сайт bouncycastle / *онлайн документація* / URL: http://bouncycastle.org (дата звернення: 11.05.2020).

References (transliterated)

1. Shanhyn V. F. *Zashchita kompyuternoy informatsii. Effektivnyye metody i sredstva*. [Protection of computer information. Effective methods and tools]. Moscow: DMK., 2010. 542 p.
2. Stelmashonok E. V., Vasilieva I. N. *Zashchita informatsii v kompyuternykh sistemakh.* [Information security in computer systems]. St. Petersburg: Piter Publ., 2017. 163 p.
3. Kosheva N. A., Maznichenko N. I., *Identifikatsiia koristuvachiv informatsiino-komp'iuternikh sistem: analiz i prognozuvannia pidkhodiv.* [Identification of information systems and computer systems: analysis and forecasting]. Kharkiv: Yaroslav Mudryi National Law University Publ., 2013. № 6. pp. 215–223.
4. Messaoud Benantar *Access Control Systems Security, Identity Management and Trust Models.* TX: Sringer Publ., 2003. 261 p.
5. Markov A. S., Tsirlov V. L. Bezopasnos dostupa: podgotovka k CISSP [Security of access: preparation for CISSP] // *Cybersecurity issues*. 2015. № 2. pp. 60–68.
6. Fadiushin A. M., Simonov V. L. Sovremennye sistemy identifikatsii lichnosti. [Modern identity identification systems.] // Modern information technologies in education, science and industry (*November 2–03, 2018, Moscow*). Moscow: Sputnik Publ., 2018. pp. 176–178.
7. Maksimenko V. N., Voloshina T. S. Analiz sistemy raspoznavaniia lits po algoritmu neironnoi seti. [Analysis of the face recognition system by the neural network algorithm]. *// economics and quality of communication systems*. 2015. № 4. pp. 31–37.
8. Gorlov V. N. Algoritmicheskie sredstva identifikatsii cheloveka po fotoportretu na osnove geometricheskikh preobrazovanii. [Algorithmic means of human identification by photo portrait based

on geometric transformations]. Collection of articles of the IV international scientific conference *(September 20, 2018, Penza)*. Penza: «Science and education» Publ., 2018. pp. 23–27.
9. Briukhomitskii Iu. A., Fedorov V. M. Metod tekstonezavisimoi identifikatsi lichnosti po golosu. [Text independent identification method by voice]. // *News SFU*, 2015. pp. 173–181.
10. Kalutskii I.V., Matiushin Iu.S., Spevakova S.V. Analiz sovremennykh staticheskikh metodov biometricheskoi identifikatsii. [Analysis of modern static methods of biometric identification] // *News of Southwestern State University*. 2019. № 1. pp. 84–94.
11. Likhachev A. E., Pavlovskii E. N., Khazankin G. R. Razrabotka sistemy identifikatsii polzovatelei kompiuternykh setei na osnove analiza ikh povedeniia. [Development of a system for identifying users of computer networks based on an analysis of their behavior]. // *Transport business*. 2017. 171 p.
12. Peregudov A. V. Klaviaturnyi pocherk kak dopolnitelnyi sposob identifikatsii polzovatelia. [Keyboard handwriting as an additional way to identify a user]. International scientific-practical conference «Research and modern education» *(March 26, 2018 Vladivostok)* Vladivostok. 2018. pp. 240–241.
13. Oleshko I. V., Gorbenko I. D. Sravnitelnyi analiz protokolov strogoi autentifikatsii [Comparative analysis of strong authentication protocols]. // *Radio engineering* 2018. № 171 pp. 198–209.
14. Sabanov A. G. Autentifikatsiia pri elektronnom obmene konfidentsialnymi dokumentami. [Authentication in the electronic exchange of confidential documents]. *TUSUR reports*. 2011. № 2. pp. 267–270.
15. Makarova I.I. Kompleksnaia informatsionnaia bezopasnost elektronnogo dokumentooborota. [Comprehensive information security of electronic document management]. // *Project management and production development: A collection of scientific papers*. – Lugansk: Dahl Severodonetsk National Institute Publ., 2004. № 3. pp.100-105.
16. L. Bass, P. Klements, R. Katsman Arkhitektura programmnogo obespecheniia na praktike [Software architecture in practice] // St. Pitersburg: Addison-Wesley Publ. –2006. 306 p.
17. Apache Tomcat official site / *online documentation* / URL: http://tomcat.apache.org (date of application: 12.04.2020).
18. MySql official site / *online documentation* / URL: http://mysql.com (date of application: 12.04.2020).
19. Java official site / *online documentation* / URL: http://java.com (date of application: 12.04.2020).
20. Bouncycastle official site / *online documentation* / URL: http://bouncycastle.org (date of application: 12.04.2020).

Надійшла (received) 14.04.2020

Відомості про авторів / Сведения об авторах / About the Authors

Батурін Єгор Леонідович – бакалавр, Національний технічний університет «Харківський політехнічний інститут», студент; м. Харків, Україна; ORCID: https://orcid.org/0000-0003-0958-6215; email: baturin.egor@ukr.net

Воловщиков Валерій Юрійович – кандидат технічних наук, доцент, Національний технічний університет «Харківський політехнічний інститут», доцент кафедри програмної інженерії та інформаційних технологій управління; м. Харків, Україна; ORCID: https://orcid.org/0000-0003-4454-2314; e-mail: valera@kpi.kharkov.ua

Шапо Владлен Феліксович – кандидат технічних наук, доцент, Національний університет «Одеська морська академія», доцент кафедри теорії автоматичного управління і обчислювальної техніки; м. Одеса, Україна; ORCID: https://orcid.org/0000-0002-3921-4159; e-mail: stani@te.net.ua

Батурин Егор Леонидович – бакалавр, Национальный технический университет «Харьковский политехнический институт», студент; г. Харьков, Украина; ORCID: https://orcid.org/0000-0003-0958-6215; email: baturin.egor@ukr.net

Воловщиков Валерий Юрьевич – кандидат технических наук, доцент, Национальный технический университет «Харьковский политехнический институт», доцент кафедри программной инженерии и информационных технологий управления; г. Харьков, Украина; ORCID: https://orcid.org/0000-0003-4454-2314; e-mail: valera@kpi.kharkov.ua

Шапо Владлен Феликсович – кандидат технических наук, доцент, Национальный университет «Одесская морская академия», доцент кафедри теории автоматического управления и вычислительной техники; г. Одесса, Украина; ORCID: https://orcid.org/0000-0002-3921-4159; e-mail: stani@te.net.ua

Baturin Yehor Leonidovich – bachelor, National Technical University “Kharkiv Polytechnic Institute”, student; Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0003-0958-6215; email: baturin.egor@ukr.net

Volovshchykov Valeriy Yuriyovich – Candidate of Technical Sciences, Docent, National Technical University “Kharkiv Polytechnic Institute”, Associate Professor of the Department of Software Engineering and Management Information Technologies; Kharkiv, Ukraine; ORCID: https://orcid.org/0000-0003-4454-2314; e-mail: valera@kpi.kharkov.ua

Shapo Vladlen Felixovitch – Candidate of Technical Sciences, Docent, National University “Odessa Maritime Academy”, Associate Professor of the Theory of Automatic Control and Computing Machinery Department; Odessa, Ukraine; ORCID: https://orcid.org/0000-0002-3921-4159; e-mail: stani@te.net.ua